

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN THE MATTER OF THE SEARCH OF:

**ONE APPLE IPHONE 14 PRO MAX,
BEARING IMEI: 35379198066465, IN A
GOLD CASE**

CURRENTLY LOCATED AT THE FBI
NORTHERN VIRGINIA RESIDENT
AGENCY IN MANASSAS, VIRGINIA.

Case No. 1:24-sw-202

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH**

I, Daniel McCoy, being duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an Application under Federal Rule of Criminal Procedure 41 for a search warrant authorizing the examination of property—an electronic device described in Attachment A (the “**SUBJECT DEVICE**”)—which is currently in law enforcement possession and the extraction from that property of the electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so employed since January 2021. I am currently assigned to the Washington Field Office, Northern Virginia Resident Agency. I am on a squad that investigates darknet related narcotics trafficking and have been assigned to this squad since June 2021. Prior to be hired as a special agent with the FBI, I was a Corporal with the Collier County Sheriff’s Office in Naples, Florida, and was so employed from April 2015 until January 2021. I have received formal training in the investigation of drug and violent crimes, including specialized training in evidence collection. I

have experience investigating various types of crime, and I have investigated or assisted in the investigation of numerous cases involving violent criminal activity, narcotics, and crimes against persons and property. I have been a sworn law enforcement officer during all times herein.

3. During my time in law enforcement, I have participated in the application for and execution of numerous arrest and search warrants in investigations of narcotics offenses, resulting in the prosecution and conviction of numerous individuals and the seizure of illegal drugs, weapons, stolen property, and other evidence of criminal activity. Through my training and experience, I am familiar with the actions, habits, traits, methods, and terminology utilized by the traffickers and abusers of dangerous controlled substances.

4. The statements in this affidavit come from my personal observations, my training and experience, information supplied to me by other law enforcement personnel, and other sources of information obtained and reviewed during the course of the investigation. This affidavit contains information necessary to support probable cause. The information contained in this affidavit is not intended to include each and every fact and matter observed by me or known to the government.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is an Apple iPhone, bearing IMEI 35379198066465, with a clear case and described in Attachment A (the “**SUBJECT DEVICE**”).

6. The **SUBJECT DEVICE** is currently located at the FBI’s Northern Virginia Resident Agency, 9325 Discovery Place, Manassas, Virginia, 20109.

7. The requested warrant would authorize the forensic examination of the **SUBJECT DEVICE** for the purpose of identifying the electronically stored data particularly described in Attachment B.

FORFEITURE LEGAL AUTHORITY

8. Title 21, United States Code, Section 853(a) (criminal forfeiture for violations of 21 U.S.C. §§ 841 and 846) provides for the forfeiture of any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation and any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation.

9. Title 21, United States Code, Section 881(a)(6) (civil forfeiture for violations of 21 U.S.C. §§ 841 and 846) provides for the forfeiture of all moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished by any person in exchange for a controlled substance or listed chemical in violation of this subchapter, all proceeds traceable to such an exchange, and all moneys negotiable instruments, and securities used or intended to be used to facilitate any violation of this subchapter.

10. Pursuant to 18 U.S.C. § 981(b) (civil seizure), property subject to civil forfeiture may be seized by a warrant issued by a judicial officer "in any district in which a forfeiture action against the property may be filed," and may be executed "in any district in which the property is found," if there is probable cause to believe the property is subject to forfeiture. A civil forfeiture action may be brought in any district where "acts or omissions giving rise to the forfeiture occurred." 28 U.S.C. § 1355(b)(1)(A).

11. Title 21, United States Code, Section 853(f) (criminal seizures) provides that the government may request a seizure warrant authorizing the seizure of property subject to forfeiture in the same manner as for a search warrant. The seizure warrant issues if the Court determines that there is probable cause to believe that the property seized would, in the event of conviction,

be subject to forfeiture and that a restraining order may not be sufficient to assure the availability of such property for forfeiture.

12. There is probable cause to believe that the cryptocurrency mentioned herein is subject to seizure and forfeiture pursuant to 21 U.S.C. § 853(a) and 21 U.S.C. § 881(a)(6) as proceeds of distribution and conspiracy to distribute controlled substances, in violation of 21 U.S.C. §§ 841 and 846.

13. I know, through my training and experience, that individuals who distribute illegal controlled substances on the darknet often use, and are paid in, cryptocurrency. Virtual currency can be stored almost anywhere, in both physical and electronic formats. For example, Attachment B lists items to be seized including bitcoin, Bitcoin wallets, Bitcoin keys, passwords, and recovery phrases. These pieces of data comprise long and complex character strings, leaving many virtual currency users to write down or otherwise record and store such items because they are too long to commit to memory. As such, these items evidencing the use of virtual currency, specifically wallets, keys, and passwords, may be documented in writing and secreted anywhere within a residence. Therefore, individuals typically keep such records, data, and documents in their residence, including in computers or on other devices that store electronic data.

14. Cryptocurrency, such as Bitcoin, serves the same purpose as United States dollars, except that it is not tied to a central bank and is not regulated by a government body such as a treasury. Cryptocurrency transactions take place entirely online and offer a degree of anonymity to users. Cryptocurrency can be maintained on custodial or non-custodial cryptocurrency wallets. Custodial wallets are typically third-party centralized exchanges. Non-custodial wallets are maintained by the owner who protects their cryptocurrency with a password or recovery phrase.¹

¹ Also known as a seed phrase.

15. The passcodes allowing users to access a bitcoin wallet, and transfer the bitcoin contained within it, may be stored on mobile devices, external or removable media, or computers. These passcodes can also be represented as long strings of characters, machine readable bar codes (QR codes), or hidden within other innocuous looking data such as image files. Private keys and “seed keys” (specialized passphrases that can be used to regenerate private keys), can also be stored on paper. Again, recovery phrases for access to electronic wallets are typically complex and are often written down or saved in an accessible manner on paper or some electronic device.

16. A recovery phrase is a series of 12–24 random words generated by the cryptocurrency wallet that grants access. Anyone who maintains the recovery phrase can access the wallet. Even if the password is lost or destroyed, the wallet can still be recreated with that recovery phrase. If both the password and the recovery phrase are lost, the wallet cannot be recovered. If law enforcement finds a recovery phrase for a wallet, it is imperative that the funds are transferred to a government-controlled wallet immediately to reduce the risk of another individual who may have the password or seed phrase accessing it remotely. For these reasons, a restraining order would be inadequate to preserve the cryptocurrency for forfeiture. By seizing the cryptocurrency and transferring it to a government-controlled wallet, the United States will prevent third parties from being able to access the cryptocurrency.

PROBABLE CAUSE

17. The United States, including the FBI, the U.S. Postal Inspection Service, and the Food and Drug Administration – Office of Criminal Investigations have been investigating a criminal enterprise utilizing the darknet to facilitate the sale of controlled substances, primarily

counterfeit Adderall² tablets made with methamphetamine.³ Throughout the investigation, law enforcement has identified at least three darknet drug vendors operating under this enterprise: MrJohnson, NuveoDeluxe, and AllStateRx. These vendors take orders for counterfeit Adderall, containing methamphetamine, over the respective darknet marketplaces (“DM”s) they operate on.⁴ Since October 2022, law enforcement has conducted over twenty (20) controlled purchases from the enterprise via the darknet. Since at least April 2022, the three darknet drug vendors have distributed more than approximately 13,000 suspected drug orders throughout the United States of America, including to the Eastern District of Virginia, using the mail. These orders have been mailed from at least three different United States federal districts, including the Middle District of Florida, the District of New Jersey, and the Eastern District of New York.

18. The investigation identified three defendants primarily linked to these individual vendor pages: JOSEPH VASQUEZ (“JOSEPH”) to vendor NuveoDeluxe, JOSHUA VASQUEZ (“JOSHUA”) to vendor AllStateRx, and RAFAEL ROMAN (“ROMAN”) to vendor MrJohnson. While each individual is primarily associated with one respective account, the investigation found significant overlaps between the three vendors and defendants demonstrating that JOSEPH, JOSHUA, and ROMAN were conspiring to sell the same product over these individual vendor pages and were sharing the proceeds of the enterprise. On February 9, 2024, a criminal complaint and arrest warrants were issued out of the Eastern District of Virginia, charging JOSEPH,

² Adderall is a brand name for a central nervous stimulant, consisting of amphetamine and dextroamphetamine, and manufactured by Teva Pharmaceuticals. Adderall is a Schedule II controlled substance, used to treat attention deficit hyperactivity disorder (“ADHD”) and narcolepsy, and only available by prescription. A popular generic form of Adderall is an oval, orange tablet with “b974” debossed on one side and “30” on the other.

³ Laboratory results for these tablets have found them to contain both “methamphetamine” and “methamphetamine (calc. as hydrochloride).”

⁴ Law enforcement was able to locate the vendor profiles for MrJohnson, NuveoDeluxe, and AllStateRx across several DMs to include Abacus, ASAP, Archetype, Tor2Door, Bohemia, and Incognito Markets.

JOSHUA, and ROMAN with conspiring to distribute 500 grams or more of a mixture or substance of methamphetamine, in violation of 21 U.S.C. §§ 841(a)(1) and 846. *See United States v. Joseph Vasquez et al*, 1:24-mj-45 (E.D. Va. Feb. 7, 2024). The affidavit from that complaint is incorporated herein by reference.

19. To summarize, law enforcement agents identified NuveoDeluxe as a significant drug vendor. Starting in May 2023, a law enforcement online covert employee (“OCE”) began purchasing counterfeit Adderall pills from NuveoDeluxe. Early purchases from NuveoDeluxe were originating from specific post offices in the Middle District of Florida. A law enforcement OCE began additional purchases from NuveoDeluxe and law enforcement agents started surveilling the common post offices in the Middle District of Florida. While surveilling these post offices, law enforcement agents were able to witness JOSEPH deposit at least one package containing an undercover order placed by the OCE from NuveoDeluxe. The tablets contained in the package were orange in color, oval in shape, with “b974” debossed on one side and “30” on the other. Subsequent laboratory analysis confirmed that these tablets contained a detectable amount of methamphetamine.

20. As part of the investigation into JOSEPH, law enforcement agents were able to identify a PO Box within the Middle District of Florida that JOSEPH opened using his issued driver’s license. At or near the time the PO Box was identified, law enforcement agents found that a 12-pound package, shipped from within the District of New Jersey, was enroute to JOSEPH at this PO Box. Law enforcement agents intercepted the package prior to delivery. On July 17, 2023, the Honorable Thomas G. Wilson, United States Magistrate for the Middle District of Florida, authorized law enforcement agents to search the package. *See* Mag. No. 8:23-mj-1863-tgw. The search found the package to contain approximately 5.5 kilograms of counterfeit Adderall tablets—

nearly 15,000 tablets in total. Specifically, these tablets were orange in color, oval in shape, with “b974” debossed on one side and “30” on the other. Subsequent laboratory analysis confirmed that these tablets contained a detectable amount of methamphetamine. These tablets were visually similar to those purchased from NuveoDeluxe and deposited into the mail by JOSEPH.

21. Law enforcement agents were able to identify through Postal records that the 5.5-kilogram package originated from a post office located at 915 Bennetts Mills Road, Jackson, New Jersey (“JACKSON POST OFFICE”). The return address on the package was listed as “Atterbury CE E, Jackson, New Jersey.” JOSHUA, who is JOSEPH’s brother, was found to live at an address on that street—721 Atterbury Court E, Jackson, New Jersey (“ATTERBURY RESIDENCE”). Physical surveillance determined that JOSHUA drove a white Jeep Grand Cherokee, bearing New Jersey license plate BB25PP (“VEHICLE 1”). A white SUV, consistent with VEHICLE 1, was seen by a local surveillance camera travelling to the JACKSON POST OFFICE shortly before the 5.5-kilogram package was mailed and then going in the opposite direction shortly after the 5.5-kilogram package was dropped off. The road where the local surveillance camera was stationed is consistent with the route one would take from the ATTERBURY RESIDENCE to the JACKSON POST OFFICE. Further, law enforcement agents reviewed USPS business records for the tracking number of the package which found that it was tracked by an IP address attributable to a telephone number linked to JOSHUA, suggesting JOSHUA mailed the 5.5-kilogram package of methamphetamine to JOSEPH.

22. Between July and September 2023, law enforcement agents found ties between NuveoDeluxe and AllStateRx that suggested the two vendors were linked. Among other ties, both vendor pages were visually similar, such as having similar layouts for their products and using a similar vendor page logo. They also advertised/sold Adderall in similar fashions, including

advertising them as “pressed,” selling the same type of orange tablet, and using overlapping return addresses. A law enforcement OCE began purchasing counterfeit Adderall from AllStateRx in September 2023. Agents conducted surveillance on JOSHUA at the ATTERBURY RESIDENCE around this time as well. On or about September 12, 2023, law enforcement agents witnessed JOSHUA leave the ATTERBURY RESIDENCE in VEHICLE 1 with a blue bag. He drove directly to the JACKSON POST OFFICE and exited VEHICLE 1 with the blue bag. He deposited several USPS Priority Mail envelopes in the USPS collection box outside the JACKSON POST OFFICE and more inside. One of the parcels that JOSHUA deposited contained an order for counterfeit Adderall that was purchased from AllStateRx by a law enforcement OCE the day prior. That parcel contained 55 tablets which were visually consistent with the tablets in the multi-kilogram package, and those received in previous undercover orders with NuveoDeluxe. Laboratory analysis confirmed these tablets contained a detectable amount of methamphetamine.

23. While discovering the connections between JOSEPH and JOSHUA, law enforcement agents were also investigating the MrJohnson vendor page, which began around October 2022. After finding that undercover parcels placed with MrJohnson were originating in Brooklyn, NY, law enforcement agents spoke with employees at several post offices in Brooklyn, NY and inquired about bulk USPS Priority Mail Envelope deposits. Employees at one post office specifically reported a male making frequent deposits of bulk items.

24. In response to the inquiries, law enforcement agents began surveilling these Brooklyn, NY post offices and, on or around September 27, 2023, law enforcement agents witnessed ROMAN deposit parcels at two different post offices in the Eastern District of New York, a short distance away from the ROMAN’s residence. One of the parcels contained an undercover order, placed by an OCE from MrJohnson. Within the parcel were numerous tablets

that were orange in color, oval in shape, with “b974” debossed on one side and “30” on the other, matching what the OCE had ordered from MrJohnson. Laboratory analysis confirmed that these tablets contained a detectable amount of methamphetamine. Out of the numerous parcels that were deposited with this undercover order, two were seized by law enforcement agents and searched pursuant to search warrants issued in the District of New Jersey. Within the parcels were numerous orange in color, oval in shape tablets with “b974” debossed on one side and “30” on the other. *See* 23-mj-12241-jbc and 23-mj-12242-jbc. These tablets were visually consistent with those previously received in undercover orders from MrJohnson, NuveoDeluxe and AllStateRx, and observed being deposited by JOSHUA and JOSEPH. Laboratory analysis confirmed that these tablets contained a detectable amount of methamphetamine.

25. As the investigation continued, it became clear that JOSEPH, JOSHUA, and ROMAN were all connected in relation to their drug activities. First, law enforcement agents conducted cryptocurrency analysis relating to the cryptocurrency wallets associated with NuveoDeluxe, AllStateRx, and MrJohnson. When law enforcement conducts investigations involving virtual currency, it sometimes uses commercial services offered by several different blockchain-analysis companies. These companies analyze the Bitcoin blockchain and attempt to identify the individuals or groups involved in transactions. Specifically, these companies have developed proprietary software that analyzes all the data underlying each Bitcoin transaction on the Bitcoin blockchain and then groups related Bitcoin transactions into “clusters” based on that analysis. The methods employed by these blockchain analysis companies have been independently validated by computer scientists, who have shown that these “clustering” techniques provide accurate results. Additionally, through numerous, unrelated investigations, law enforcement has been able to corroborate the accuracy of the information provided via these third-party services.

26. Throughout the investigation, law enforcement applied cryptocurrency analysis to determine the flow of proceeds from and to each individual vendor. It is common in darknet drug investigations for individuals involved with darknet vendors to utilize cryptocurrency to attempt to obscure their involvement with the vendor pages. This investigative strategy also uses intelligence gathered from other law enforcement investigations, which can include access to DM data. Utilizing these sophisticated investigative techniques, law enforcement identified several cryptocurrency wallets which received payments believed to be associated with MrJohnson (“MRJOHNSON WALLET”), NuveoDeluxe (“NUVEODELUXE WALLET”), and AllStateRx (“ALLSTATERX WALLET”).⁵

27. Regarding the NUVEODELUXE WALLET, law enforcement found that it continuously made payments to a Bitcoin exchange platform, which exchanges cryptocurrency for gift cards at popular retailers (“EXCHANGE BUSINESS 1”). In response to a request from law enforcement, EXCHANGE BUSINESS 1 provided information for those transactions, which found that payments initiated from the NUVEODELUXE WALLET ultimately were used to purchase gift cards which were redeemed by JOSEPH in his name. For these reasons, law enforcement believes JOSEPH controls the NUVEODELUXE WALLET.

28. Regarding the ALLSTATERX WALLET, law enforcement found that it also made payments to EXCHANGE BUSINESS 1 for gift cards. In response to a subpoena, EXCHANGE BUSINESS 1 provided information for those transactions, which found payments initiated from the ALLSTATERX WALLET were redeemed by JOSHUA and his live-in partner (“UCC-1”) in their names. In response to a subpoena, it was found that an IP address attributed to a telephone

⁵ For purposes of clarity and continuity, the several cryptocurrency wallets associated with each vendor are referred to as a single unit.

number associated with JOSHUA was used for several of these orders. For these reasons, law enforcement believes JOSHUA controls the ALLSTATERX WALLET.

29. Further analysis found that cryptocurrency was continuously being transferred between the NUVEODELUXE WALLET and ALLSTATERX WALLET. The analysis has shown that, to date, NUVEODELUXE WALLET and the ALLSTATERX WALLET have transferred over \$130,000 in Bitcoin between each other. The most recent payment was for approximately \$9,000 in cryptocurrency on or about January 12, 2024. Based on JOSEPH's connections to the NUVEODELUXE WALLET and JOSHUA's connections to the ALLSTATERX WALLET, law enforcement believes that JOSEPH and JOSHUA were directly involved in these transfers.

30. Since June 2022 through the arrests of the defendants, law enforcement discovered that the MRJOHNSON WALLET conducted transactions totaling over \$1,000,000 worth of Bitcoin while utilizing several other Bitcoin wallets associated with the MRJOHNSON WALLET (the "ASSOCIATE WALLETS"). Further analysis found a pattern of payments from MrJohnson being sent to the ASSOCIATE WALLETS and ultimately into accounts at a financial institution that operates a mobile payment application ("PAYMENT SERVICE 1").⁶ Records from PAYMENT SERVICE 1 indicate that at least one of the accounts was registered to ROMAN using an IP address attributed to ROMAN's residence, suggesting ROMAN controls some of the ASSOCIATE WALLETS.

⁶ PAYMENT SERVICE 1 enables users to make retail payments using a smartphone, to send payments peer-to-peer to other users, and to buy and sell cryptocurrency for US currency, among other services.

31. Finally, from at least August to mid-September 2023,⁷ the cryptocurrency analysis found that the MRJOHNSON WALLET, the NUVEODELUXE WALLET, and the ALLSTATE RX WALLET all sent cryptocurrency to the ASSOCIATE WALLETS. During this period, the ASSOCIATE WALLETS ultimately sent cryptocurrency to the same PAYMENT SERVICE 1 accounts accessed at ROMAN's residence and believed to be used by ROMAN.

32. Law enforcement believes the cryptocurrency wallets above are used exclusively for proceeds from illegal drug activity. Law enforcement reviewed income records for JOSEPH, JOSHUA, and ROMAN, which have reported to their respective states. None of the three individuals have reported levels of income that would explain the financial amounts involved above. Specifically, since the investigation began in 2022, ROMAN had no reportable income, JOSEPH had no reportable income,⁸ and JOSHUA earned \$10,370.

I. Search Warrants and Arrests of ROMAN, JOSEPH, and JOSHUA

33. On February 15, 2024, five search warrants were sworn out of the Eastern District of New York for locations law enforcement found were tied to the conspiracy. On the same day, three search warrants were sworn out of the District of New Jersey for locations law enforcement found were tied to the conspiracy.

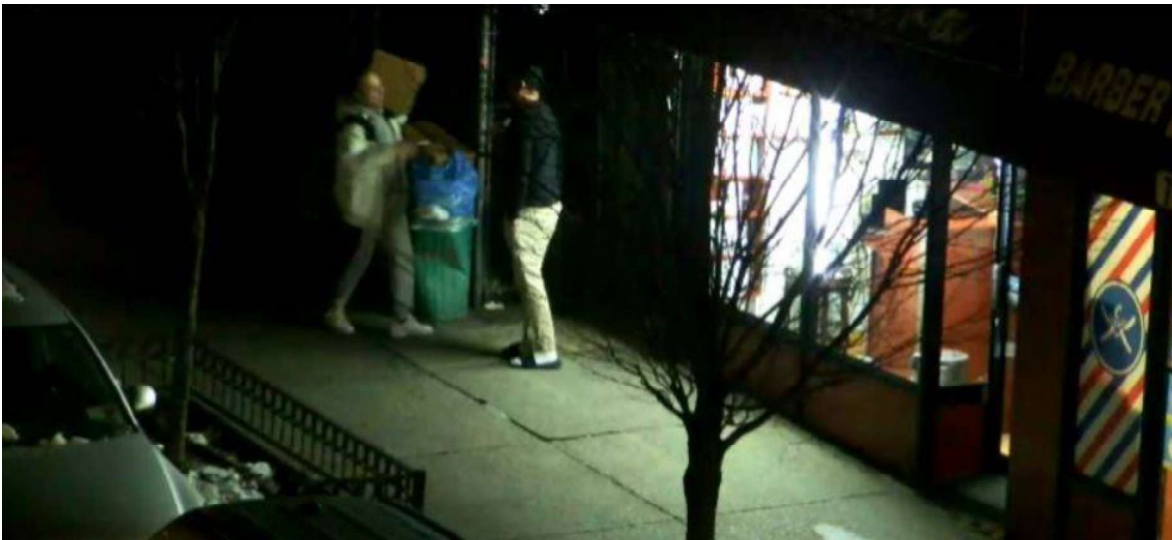
34. On February 21, 2024, six search warrants were executed, as well as the three arrest warrants for JOSEPH, JOSHUA, and ROMAN.

⁷ Subpoenas to PAYMENT SERVICE 1 for time periods after mid-September 2023 are still outstanding. However, law enforcement is still able to determine through its analysis that cryptocurrency is being sent from the ASSOCIATE WALLETS to PAYMENT SERVICE 1 after mid-September 2023. Therefore, law enforcement believes that the accounts at PAYMENT SERVICE 1 attributed to ROMAN are still receiving cryptocurrency from the ASSOCIATE WALLETS.

⁸ JOSEPH recently began driving for a popular ride sharing service, though there is still no reportable income to either Florida, New York, or New Jersey.

a. Search of Xiara's Beauty Salon & Barber Shop

35. Throughout the investigation, ROMAN, JOSHUA, and others, known and unknown, were found to be associated with Xiara's Beauty Salon & Barbershop in the Eastern District of New York. For example, on or about January 15, 2024, surveillance located JOSHUA and ROMAN outside of the Xiara's Beauty Salon & Barbershop, then entering the basement. ROMAN was observed carrying a large box, as shown below:



36. On or about February 15, 2024, the Honorable Vera M. Scanlon, United States Magistrate Judge for the Eastern District of New York, authorized law enforcement to search Xiara's Beauty Salon & Barbershop. *See* 24-mj-140-vms. On or about February 21, 2024, law enforcement executed that search warrant, and, amongst other items, located two tablet press machines, as shown below:



37. Law enforcement also seized approximately 50,000 suspected methamphetamine tablets. These tablets were orange in color, oval in shape, and debossed with “b974” on one side and “30” on the other. These tablets were visually similar to those sold by NuveoDeluxe, AllStateRx, and MrJohnson, and those seen deposited at post offices by JOSEPH, JOSHUA, and ROMAN throughout the investigation and similar to the 5.5-kilogram package law enforcement believes JOSHUA mailed to JOSEPH. The seized tablets are shown below:





b. Search of ROMAN's Residence

38. On February 15, 2024, the Honorable Vera M. Scanlon, United States District Judge for the Eastern District of New York, authorized law enforcement to search a location the investigation found was ROMAN's residence. *See* 24-mj-140-vms. JOSHUA had been seen at ROMAN's residence several times throughout the investigation. On or about February 21, 2024, law enforcement searched Roman's residence. Amongst other items seized were numerous suspected methamphetamine tablets which were orange in color, oval in shape, and debossed with "b974" on one side and "30" on the other, similar to those sold by NuveoDeluxe, AllStateRx, and MrJohnson. The tablets were packaged for distribution, as shown below:



c. Search of the ATTERBURY RESIDENCE

39. On or about February 15, 2024, the Honorable Rukhsanah L. Singh, United States Magistrate Judge for the District of New Jersey, authorized law enforcement to search the ATTERBURY RESIDENCE. *See* 24-mj-14014-rls. On or about February 21, 2024, law enforcement executed the search warrant. Amongst other items, law enforcement located numerous heat and vacuum sealed bags and postage labels, and nearly \$300,000 in cash. Notably, JOSHUA and UCC-1 have no reported income that would explain the large amount of cash seized.

d. Arrest of ROMAN, JOSEPH, JOSHUA, and the Seizure of the SUBJECT DEVICE

40. JOSEPH, JOSHUA, and ROMAN were all arrested on February 21. After ROMAN was arrested, he gave a voluntary, post-*Miranda* interview. Among other things, he admitted he was paid in cryptocurrency to work for JOSHUA and to purchase items on the Internet to further the conspiracy's drug distribution.

41. Throughout the investigation, JOSEPH primarily lived and operated out of Florida. However, shortly before JOSEPH's arrest on February 21, law enforcement learned that JOSEPH had relocated to Brooklyn, New York. To locate and execute the arrest warrant issued for JOSEPH, as described in paragraph 18, the Honorable William E. Fitzpatrick authorized law enforcement to receive location data from T-Mobile for JOSEPH's telephone, the **SUBJECT DEVICE**. *See* 1:24-sw-91-wef. On the same day the warrant was issued, T-Mobile informed law enforcement that the **SUBJECT DEVICE** was located in New York City. Data from the **SUBJECT DEVICE** showed that it was consistently in contact with JOSHUA, JOSEPH's brother and one of his co-defendants.

42. On or about 7:17 PM on February 18, 2024, location data showed the **SUBJECT DEVICE** was located in the Longwood neighborhood of the Bronx in New York City. Law enforcement traveled to this area and located JOSEPH standing outside of his vehicle, as shown below. Once JOSEPH departed in the vehicle, the GPS pings on the **SUBJECT DEVICE** showed it to travel as well.



43. On or about February 19, 20224, GPS pings showed the **SUBJECT DEVICE** to be in the area of 3025 W 32nd Street, Brooklyn, New York. JOSEPH's mother, Linda Serrano ("SERRANO") lives in apartment 11E in this building. This address is also listed on JOSEPH's driver's license. Law enforcement responded to this area and located JOSEPH's vehicle parked outside of the building. At approximately 12:40 PM on the same day, JOSEPH exited the building, entered the vehicle, and departed, as shown below. As JOSEPH departed, GPS pings for the **SUBJECT DEVICE** showed it to travel as well.

44. On or about 6:00 AM on February 21, 2024, GPS pings for the **SUBJECT DEVICE** showed it again to be in the area of 3025 W 32nd Street, Brooklyn, New York. Law enforcement subsequently located and arrested JOSEPH at the SERRANO's apartment, 11E, in that building. However, due to a miscommunication with the local team that arrested JOSEPH, law enforcement did not seize the **SUBJECT DEVICE** during JOSEPH's arrest.

45. On or about March 4, 2024, law enforcement made contact with SERRANO at her residence, where JOSEPH was arrested. SERRANO explained that she recently allowed JOSEPH to stay at her residence after he came back to New York from Florida due to a recent breakup with his girlfriend. SERRANO was aware that JOSEPH had her address listed as his own on his driver's license, but he had not lived there for a period of time.

46. To minimize any damage to JOSEPH's vehicle during the execution of a search warrant on his vehicle, law enforcement asked if SERRANO had the keys to the vehicle. SERRANO did not have the keys to the vehicle, but did have multiple driver's licenses in JOSEPH's name, multiple credit cards in JOSEPH's name, and the **SUBJECT DEVICE**. While law enforcement intended to ask consent to seize the **SUBJECT DEVICE** while at SERRANO's

residence, SERRANO offered the items to law enforcement on her own accord before law enforcement asked for the **SUBJECT DEVICE**, stating she did not want the items in her house.

47. To ensure that this was indeed the **SUBJECT DEVICE**, law enforcement called the telephone number for the **SUBJECT DEVICE**. After it rang, confirming it was the **SUBJECT DEVICE**, it was placed into airplane mode in order to preserve the contents of the device. Based on my training and experience, I know that the **SUBJECT DEVICE** has been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state that they were when the **SUBJECT DEVICE** first came into possession of the FBI. The **SUBJECT DEVICE** was transported to the Eastern District of Virginia on or about March 4, 2024, and has remained in the Eastern District of Virginia since. On March 23, 2024, I confirmed with SERRANO that the **SUBJECT DEVICE** had not been accessed or tampered with between the arrest of JOSEPH and law enforcement taking possession of the device on March 4.

USE OF CELLULAR DEVICES AND CRYPTOCURRENCY BY DRUG TRAFFICKERS

48. Based on my training, experience, knowledge, participation in narcotics investigations, and the training and experience of other agents and detectives with whom I am working closely in this investigation, I also know that drug traffickers use cell phones in furtherance of drug trafficking, and I am familiar with the methods used by individuals involved in the distribution of narcotics and drug trafficking. I also know that drug traffickers on the darknet often use cryptocurrency. In particular, I know that:

- a. Narcotics traffickers frequently use cellular telephones to further their illegal activities by, among other things, remaining in constant or ready communication with one another without restricting either party to a particular location at which they might be subject to physical surveillance by law enforcement authorities. Narcotics traffickers rarely refer to methamphetamine or other illegal drugs expressly by name. Instead, to conceal the true nature of their illegal activities and to thwart detection by law enforcement, narcotics traffickers routinely refer to drugs, drug quantities, and drug prices by using seemingly innocuous words or

phrases. I have become familiar the methods, language, and terms that narcotics traffickers use to disguise conversations about their narcotics activities.

- b. Drug traffickers frequently have access to several cellular telephones, and that they periodically use newly acquired cellular telephones, all in an effort to avoid detection and to impede law enforcement efforts. Drug traffickers also communicate by use of text messaging to discuss types, quantities, and prices of narcotics, as well as to discuss meeting locations, all in an effort to elude detection and to impede the efforts of law enforcement. Drug dealing is an ongoing process that requires the development, use, and protection of a communications network to facilitate daily narcotics distribution.
- c. To that end, drug traffickers use communication facilities (including cell phones) to further every aspect of the drug trade. Drug traffickers use communication facilities to contact—by way of both voice call and electronic message—drug suppliers, customers, and coconspirators, all for the purpose of acquiring, storing, transporting, and distributing drugs. Drug traffickers also maintain, on their cell phones, records related to drug distribution (e.g., ledgers and notes pertaining to drug sales), and photographs of drugs, drug paraphernalia, and the instruments of the drug trade. Further, the location data associated with a drug trafficker’s cell phones assists investigators in identifying the drug trafficker’s residence, stash house, coconspirators, the residences of the trafficker’s coconspirators, and meeting locations.
- d. For investigations where drug traffickers rely on the United States Postal Service (“USPS”), and other parcel carriers, small package carriers, and common carriers to ship/transport quantities of illicit narcotics, I am aware that recipients and shippers alike use their cellular devices to check tracking numbers and shipping information for the illicit packages. They also use various addresses, to include locations where they do not reside, in order to avoid detection by law enforcement.
- e. Individuals who distribute illegal controlled substances on the darknet often use and are paid in virtual currency which is also known as cryptocurrency. Virtual currency could be stored almost anywhere within a location, in both physical and electronic formats. For example, Attachment B lists items to be seized including cryptocurrency, cryptocurrency wallets, Bitcoin keys, and passwords. These pieces of data compromise long and complex character strings, and in my training and experience I know that many virtual currency users write down or otherwise record and store such items because they are too long to commit to memory. As such, these items evidencing the sale of virtual currency, specifically wallets, keys, and passwords may be documented in writing and secreted anywhere within a residence. Therefore, individuals typically keep such records, data and documents in their residence, including in computers or on other devices that store electronic data.

49. Relevant here, throughout the investigation the defendants have utilized several different telephone numbers in furtherance of the conspiracy. For instance, JOSHUA has operated multiple telephone numbers on several different devices including, but not limited to, XXX-XXX-8030, XXX-XXX-0032, and XXX-XXX-8179. Several of these numbers have been directly tied to the drug activity in the conspiracy. For instance, when the 5.5-kilogram package was mailed, law enforcement reviewed USPS business records for the tracking number of the package which found that it was tracked by both the XXX-XXX-0032 and XXX-XXX-8179 numbers.

50. JOSEPH has operated multiple telephone numbers on several different devices including XXX-XXX-6091, XXX-XXX-3019, XXX-XXX-5462, and the **SUBJECT DEVICE**, to name a few. Based on my training and experience, such frequent use of telephone numbers in a short time suggests JOSEPH changed telephone numbers to avoid detection by law enforcement. Since the conspiracy was carried out primarily over the Internet and used cryptocurrency, which can be accessed and transferred by cell phones, as proceeds, I believe there is probable cause that the **SUBJECT DEVICE** contains the items and evidence listed in Attachment B.

TECHNICAL TERMS

51. Based on my training and experience, I know the following technical terms are commonly used to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and

moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving

them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

52. Based on my training and experience, I know that the **SUBJECT DEVICE**, an Apple iPhone 14, has the capability to allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

53. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

54. There is probable cause to believe that things that were once stored on the **SUBJECT DEVICE** may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a device or storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a device or storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, electronic storage media—in particular, an electronic device’s internal hard drive—contain electronic evidence of how an electronic device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. User typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

55. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT DEVICE** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **SUBJECT DEVICE** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

56. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **SUBJECT DEVICE** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

57. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

//

//

//

//

//

//

//

//

//

//

//

CONCLUSION

I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **SUBJECT DEVICE**, further described in Attachment A, to seek the items and information further described in Attachment B.

Respectfully submitted,

Daniel McCoy

Daniel McCoy
Special Agent
Federal Bureau of Investigation

Attested to in accordance with the requirements of
Fed. R. Crim. P. 4.1 via telephone on March 25, 2024.

Lindsey R Vaala Digitally signed by Lindsey R
Vaala
Date: 2024.03.25 13:16:30 -04'00'

The Honorable Lindsey R. Vaala
United States Magistrate Judge
Alexandria, Virginia

ATTACHMENT A

Items To Be Searched

The property to be searched is an Apple iPhone 14 Pro Max, bearing IMEI 35379198066465, in a gold case, currently located at the FBI Northern Virginia Resident Agency, 9325 Discovery Boulevard, Manassas, Virginia (the “**SUBJECT DEVICE**”). The front of the **SUBJECT DEVICE** is a picture of JOSEPH holding several one-hundred-dollar bills.

The SUBJECT DEVICE



ATTACHMENT B

Items To Be Seized

1. All records on the **SUBJECT DEVICE** described in Attachment A that relate to the violations of Title 21, United States Code, Sections 841(a)(1) and 846, that involve JOSHUA, JOSEPH, ROMAN, and others, both known and unknown, including but not limited to:
 - a. Any conversations, whether through text messages or other applications, where JOSEPH or others discuss controlled substances;
 - b. Lists of customers and related identifying information;
 - c. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions,
 - d. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
 - e. Any photographs or videos of controlled substances;
 - f. All bank records, checks, credit card bills, account information, and other financial records;
 - g. All records pertaining to travel (including but not limited to: documentation pertaining to air travel, hotel/rental property accommodations, rental vehicles, or any other mode of transportation);
 - h. Any information related to the shipment or mailing of parcels (including but not limited to: receipts, delivery notices, and other shipping documentation from the U.S. Postal Service, small package carriers, or common carriers which indicate the shipment of packages and parcels containing controlled substances, any other records of shipments of parcels, notes recording the tracking number/ information

of parcels, photographs of parcels or their labels, photographs documenting the tracking number/ information of parcels, payment receipts related to parcels, documents or information pertaining to shipping label creation or the payment for shipping of parcels);

- i. Password, encryption keys, PGP keys, recovery seeds, and other access devices that may be necessary to access devices;
 - j. Records of or information about Internet Protocol addresses used by the device;
 - k. Evidence of the use of virtual private networks and the TOR network, including, but not limited to, access of darknet marketplaces;
 - l. Records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
2. Evidence of user attribution showing who used or owned the **SUBJECT DEVICE** at the time the things described in this warrant were created, edited, deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.
3. Any and all cryptocurrency, to include the following:
- a. Any and all representations of cryptocurrency public keys or addresses;
 - b. Any and all representations of cryptocurrency private keys; and
 - c. Any and all representations of cryptocurrency wallets or their constitutive parts, to include "recover seeds" or "root keys" which may be used to regenerate a wallet.

4. The United States is authorized to seize any and all cryptocurrency by transferring the full account balance in each wallet to a public cryptocurrency address controlled by the United States.

5. The United States is further authorized to copy any wallet files and restore them onto computers controlled by the United States. By restoring the wallets on its own computers, the United States will continue to collect cryptocurrency transferred into the wallets seized as a result of transactions that were not yet completed at the time that the devices were seized.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized materials that are potentially attorney-client privileged or subject to the work-product doctrine (“Protected Materials”), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team

will review seized communications and segregate potential Protected Materials. At no time will the Filter Team advise the Prosecution Team of the substance of any potential Protected Materials. The Filter Team then will provide all communications that are not potential Protected Materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potential Protected Materials are not protected, the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potential Protected Materials to the Prosecution Team. The investigative team may continue to review any information not segregated as potentially privileged.